PATENT ABSTRACTS OF JAPAN

(11)Publication number : **06-224896**
(43)Date of publication of application : **12.08.1994**

(51)Int.Cl. **H04L 9/00**
H04L 9/10
H04L 9/12
G09C 1/00

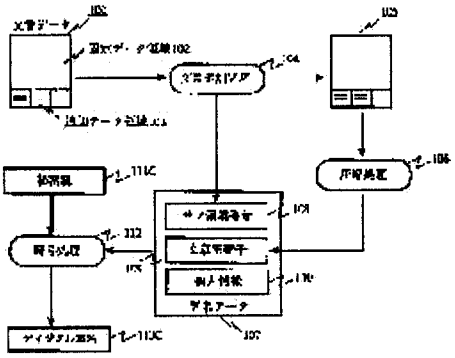
(21)Application number : **05-303773**
(22)Date of filing : **03.12.1993**

(71)Applicant : **HITACHI LTD**
HITACHI CHUBU SOFTWARE LTD
(72)Inventor : **MATSUMOTO HIROSHI**
TAKARAGI KAZUO
SUZAKI SEIICHI
MAEZAWA HIROYUKI
KOIZUMI SHINOBU

(30)Priority
Priority number : **04350461** Priority date : **03.12.1992** Priority country : **JP**

(54) ELECTRONIC DOCUMENT PROCESSING SYSTEM AND PREPARING METHOD FOR DIGITAL SIGNATURE

(57)Abstract:
PURPOSE: To provide the preparing method for digital signature and an authentication method for electronic document so as to change document contents on the way of circulation.
CONSTITUTION: When a user adds or changes received document contents at a terminal equipment 10 receiving the electronic document to which the digital signature is added, signature data 107 containing version management information 108 required for restoring an electronic document 101 of a previous version from an electronic document 105 of a new version are processed in ciphering by a secret key 111 of the user so as to prepare the digital signature 113 of the user. Since the document provided with the version preceded by one version from the received document is restored by using version management information 208 contained in signature data 207 obtained by decoding the last digital signature by a public key 208, at the terminal equipment receiving the electronic document, the relation of correspondence between all the digital signatures and documents can be confirmed by the similar procedure.



LEGAL STATUS

[Date of request for examination]	05.04.2000
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	3260524
[Date of registration]	14.12.2001
[Number of appeal against examiner's decision of	

rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right] 14.12.2004

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平6－224896

(43)公開日　平成６年(1994)８月12日

(51)Int.Cl.[5]		識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ０４Ｌ	9/00				
	9/10				
	9/12				
Ｇ０９Ｃ	1/00		8837－5L		
			7117－5K	Ｈ０４Ｌ　9/ 00　Ｚ	

審査請求　未請求　請求項の数18　ＯＬ　（全 22 頁）

(21)出願番号　特願平5－303773

(22)出願日　平成５年(1993)12月３日

(31)優先権主張番号　特願平4－350461

(32)優先日　平４(1992)12月３日

(33)優先権主張国　日本（ＪＰ）

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(71)出願人　000233457
日立中部ソフトウェア株式会社
愛知県名古屋市中区栄３丁目10番22号

(72)発明者　松本　浩
愛知県名古屋市中区栄三丁目10番22号　日立中部ソフトウェア　株式会社内

(72)発明者　宝木　和夫
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(74)代理人　弁理士　小川　勝男

最終頁に続く

(54)【発明の名称】　電子化文書処理システムおよびディジタル署名の生成方法

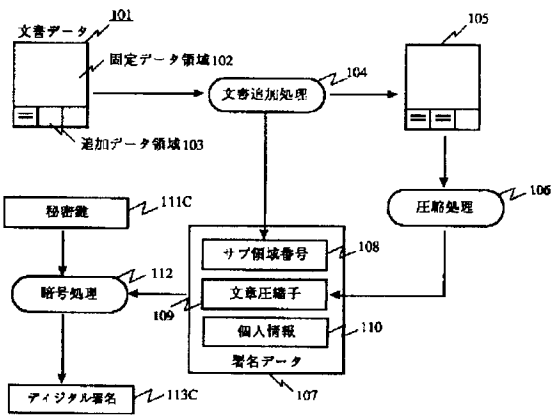
(57)【要約】

【目的】　回覧途中で文書内容の変更を可能にしたディジタル署名の生成方法と電子化文書の認証方法を提供する。

【構成】　ディジタル署名が付された電子化文書を受け取った端末装置１０で、ユーザが受信文書内容に追記または変更を行なった場合に、新バージョンの電子化文書１０５から前バージョンの電子化文書１０１を復元するために必要なバージョン管理情報１０８を含む署名データ１０７をユーザの秘密鍵１１１で暗号化処理することによって、上記ユーザのディジタル署名１１３を生成する。

【効果】　電子化文書を受信した端末装置では、最後のディジタル署名を公開鍵２１１で復号化して得られた署名データ２０７に含まれるバージョン管理情報２０８を用いて、受信文書から１つ前のバージョンをもつ文書を復元できるため、同様の手順で、全てのディジタル署名について文書との対応関係を確認できる。

図　1



1

【特許請求の範囲】

【請求項１】少なくとも１つのディジタル署名が関係付けられている前バージョンの電子化文書について、文書データの追記または変更を行なって新バージョンの電子化文書を作成し、

上記新バージョンの電子化文書を圧縮処理して文書の圧縮子を生成し、

上記文書圧縮子と、署名者の個人情報と、上記新バージョンの電子化文書から上記前バージョンの電子化文書を復元するために必要なバージョン管理情報とを含む署名データを暗号化処理して、新たなディジタル署名を生成し、

上記新バージョンの電子化文書に、上記前バージョンの電子化文書に関係付けられていたディジタル署名と上記新たなディジタル署名とを関係付けることを特徴とするディジタル署名の生成方法。

【請求項２】前記署名データの暗号化処理が、公開鍵暗号化法において前記署名者に割り当てられた秘密鍵を用いて行われることを特徴とする請求項１に記載のディジタル署名の生成方法。

【請求項３】前バージョンの電子化文書が、データを追記するために用意された予め定義された複数の部分領域を有し、前記新バージョンの電子化文書が、前バージョンの電子化文書中の上記部分領域の１つに文書データを新たに追記することによって生成され、前記バージョン管理情報は、文書データが新たに追記された上記部分領域の１つを特定するための情報からなることを特徴とする請求項１に記載のディジタル署名の生成方法。

【請求項４】前記文書圧縮子が、前記新バージョンの電子化文書中の前記複数の部分領域に含まれる文書データを圧縮処理して得られる第１の圧縮子と、前記新バージョンの電子化文書中のその他の領域に含まれる文書データを圧縮処理して得られる第２の圧縮子とからなることを特徴とする請求項３に記載のディジタル署名の生成方法。

【請求項５】前記新バージョンの電子化文書が、前バージョンの電子化文書中の少なくとも１つの部分領域での新文書データの挿入または既存文書データの削除を行うことによって生成され、前記バージョン管理情報が、上記部分領域の位置と、前バージョンの電子化文書から削除された文書データおよび挿入された新文書データを特定するための情報とからなることを特徴とする請求項１に記載のディジタル署名の生成方法。

【請求項６】少なくとも１つのディジタル署名が関係付けられている前バージョンの電子化文書について文書データの追記または変更を行ない、新バージョンの電子化文書を作成し、

上記新バージョンの電子化文書を圧縮処理して第１の圧縮子を生成し、

上記新バージョンの電子化文書から上記前バージョンの

2

電子化文書を復元するために必要なバージョン管理情報を圧縮処理して第２の圧縮子を生成し、

上記第１の圧縮子と、上記第２の圧縮子と、署名者の個人情報とを含む署名データを暗号化処理して新たなディジタル署名を生成し、

上記新バージョンの電子化文書に、上記バージョン管理情報と、上記前バージョンの電子化文書に関係付けられていたディジタル署名と、上記新たなディジタル署名とを関係付けることを特徴とする電子化文書に付すべきディジタル署名の生成方法。

【請求項７】前記署名データの暗号化処理が、公開鍵暗号化法において前記署名者に割り当てられた秘密鍵を用いて行われることを特徴とずる請求項６に記載の電子化文書に付すべきディジタル署名の生成方法。

【請求項８】前記新バージョンの電子化文書が、前バージョンの電子化文書中の少なくとも１つの部分領域での新文書データの挿入または既存文書データの削除を行うことによって生成され、前記バージョン管理情報が、上記部分領域の位置と、前バージョンの電子化文書から削除された文書データおよび挿入された新文書データを特定するための情報とからなることを特徴とする請求項６に記載の電子化文書に付すべきディジタル署名の生成方法。

【請求項９】前記新バージョンの電子化文書と対をなして複数のレコードからなるテーブルを有し、上記テーブルの各レコードが、各署名者の識別子と、前記バージョン管理情報と前記各ディジタル署名の少なくとも一方を記憶することを特徴とする請求項８に記載の電子化文書に付すべきディジタル署名の生成方法。

【請求項１０】所定の順序で付された複数のディジタル署名を伴う電子化文書の認証方法において、

上記ディジタル署名のうちの少なくとも１つが、署名者の個人情報と、該ディジタル署名と対応するバージョンの電子化文書を圧縮処理して得られた圧縮子と、該ディジタル署名と対応するバージョンの電子化文書から前バージョンの電子化文書を復元するために必要なバージョン管理情報とを含む署名データを暗号化して得たものであり、

（ａ）上記受信メッセージに含まれる電子化文書をチェック対象文書として、チェック対象文書に所定の圧縮処理を施して圧縮子を生成し、

（ｂ）上記受信メッセージに含まれるディジタル署名のうち最新のものから順にチェック対象として選び、チェック対象となったディジタル署名の署名者と対応する復号鍵を用いて、該チェック対象ディジタル署名から署名データを復号し、　（ｃ）上記復号された署名データから抽出された圧縮子と、上記チェック対象文書の圧縮子とが一致するか否かを検査し、

（ｄ）上記復号された署名データがバージョン管理情報を含む場合、該バージョン管理情報と上記チェック対象

3

文書とから、前バージョンの電子化文書を復元し、上記前バージョンの電子化文書と次のディジタル署名をそれぞれ新たなチェック対象文書およびチェック対象ディジタル署名として、ステップ（ａ）～（ｃ）を繰り返し、もし、上記復号された署名データがバージョン管理情報を含まない場合は、次のディジタル署名をチェック対象ディジタル署名としてステップ（ｂ）～（ｃ）を繰り返すことを特徴とする電子化文書の認証方法。

【請求項１１】前記ステップ（ｂ）で行う前記署名データの復号を、公開鍵暗号法における前記署名者と対応する公開鍵を用いて行うことを特徴とする請求項１０に記載の電子化文書の認証方法。

【請求項１２】前記ステップ（ｄ）で行う前記前バージョンの電子化文書の復元を、前記チェック対象文書から、前記バージョン管理情報が特定する部分領域の文書情報を削除することによって行うことを特徴とする請求項１０に記載の電子化文書の認証方法。

【請求項１３】所定の順序で付された複数のディジタル署名と、１つのバージョンの電子化文書から前バージョンの電子化文書を復元するために必要なバージョン管理情報とを伴う電子化文書の認証方法において、

上記ディジタル署名のうちの少なくとも１つが、署名者の個人情報と、該ディジタル署名と対応するバージョンの電子化文書を圧縮処理して得られた第１の圧縮子と、該ディジタル署名と対応するバージョン管理情報を圧縮処理して得られた第２の圧縮子とを含む署名データを暗号化して得たものであり、

（ａ）上記受信メッセージに含まれる電子化文書をチェック対象文書として、該チェック対象文書に所定の圧縮処理を施して圧縮子を生成し、

（ｂ）上記受信メッセージに含まれるディジタル署名を最新のものから順にチェック対象として選び、チェック対象となったディジタル署名の署名者と対応する復号鍵を用いて、該チェック対象ディジタル署名から署名データを復号し、

（ｃ）上記復号された署名データから抽出された第１の圧縮子と、上記チェック対象文書の圧縮子とが一致するか否かを検査し、

（ｄ）上記復号された署名データが第２の圧縮子を含む場合、上記受信メッセージに含まれるバージョン管理情報を最新のものから順にチェック対象管理情報として選び、該チェック対象管理情報に所定の圧縮処理を施して得られた圧縮子と上記第２の圧縮子とが一致するか否かを検査し、

（ｅ）上記復号された署名データが第２の圧縮子を含む場合、上記チェック対象となったバージョン管理情報と上記チェック対象文書とから、前バージョンの電子化文書を復元し、上記前バージョンの電子化文書と次のディジタル署名をそれぞれ新たなチェック対象文書およびチェック対象ディジタル署名として、ステップ（ａ）～

4

（ｄ）を繰り返し、もし、上記復号された署名データがバージョン管理情報を含まない場合は、次のディジタル署名をチェック対象ディジタル署名としてステップ（ｂ）～（ｄ）を繰り返すことを特徴とする電子化文書の認証方法。

【請求項１４】前記ステップ（ｂ）で行う前記署名データの復号に、公開鍵暗号法における前記署名者と対応する公開鍵を用いることを特徴とする請求項１０に記載の電子化文書の認証方法。

【請求項１５】少なくとも１つのディジタル署名と前バージョンの電子化文書とを含む通信メッセージをネットワークから受信するための手段と、

上記ネットワークから受信した前バージョンの電子化文書とそれに付されたディジタル署名との関係をチェックするための検査手段と、

ユーザからの入力操作に応じて、上記前バージョンの電子化文書に部分的な変更または情報追加を行い、新バージョンの電子化文書を生成するための手段と、

上記新バージョンの電子化文書と所定の関係をもつ新たなディジタル署名を生成するための手段と、

上記新バージョンの電子化文書と、前バージョンの電子化文書と共に受信したディジタル署名と、上記新たなディジタル署名とを含む通信メッセージを上記ネットワークに送信するための手段とを有し、

上記ディジタル署名生成手段が、上記新バージョンの電子化文書を圧縮処理して得られた文書圧縮子と、上記ユーザの個人情報と、上記新バージョンの電子化文書から上記前バージョンの電子化文書を復元するために必要なバージョン管理情報とからなる署名データを、上記ユーザの秘密鍵で暗号化処理することによって、上記新たなディジタル署名を生成することを特徴とする電子化文書の処理システム。

【請求項１６】前記検査手段が、

上記受信メッセージに含まれる電子化文書をチェック対象文書として、該チェック対象文書に所定の圧縮処理を施して文書圧縮子を生成する第１手段と、

上記受信メッセージに含まれるディジタル署名のうち、最新のものから順にチェック対象として選ばれたディジタル署名から、これと対応する復号鍵を用いて署名データを復号する第２手段と、

上記復号された署名データから抽出された文書圧縮子と、上記チェック対象文書から生成された文書圧縮子とが一致するか否かを検査する第３手段と、

上記復号された署名データがバージョン管理情報を含む場合、該バージョン管理情報と上記チェック対象文書とに基づいて、前バージョンの電子化文書を復元する第５手段とを有し、

上記前バージョンの電子化文書を新たなチェック対象文書として、上記第１手段～第４手段を動作させることを特徴とする請求項１５に記載の電子化文書の処理システ

5

ム。

【請求項17】ネットワークから、電子化文書と、少なくとも1つのディジタル署名を含む文書付属情報とを有する通信メッセージを受信するための手段と、

上記ネットワークから受信した前バージョンの電子化文書とそれに付されたディジタル署名との関係をチェックするための検査手段と、

ユーザからの入力操作に応じて、上記前バージョンの電子化文書に部分的な変更または情報追加を行い、新バージョンの電子化文書を生成するための手段、

上記新バージョンの電子化文書と所定の関係をもつ新たなディジタル署名を生成するための手段と、

上記新バージョンの電子化文書と、前バージョンの電子化文書と共に受信した文書付属情報と、上記新たなディジタル署名と、上記バージョン管理情報とを含む通信メッセージを上記ネットワークに送信するための手段とを有し、

上記ディジタル署名が、上記新バージョンの電子化文書を圧縮処理して得られた第1の圧縮子と、上記ユーザの個人情報と、上記新バージョンの電子化文書から上記前バージョンの電子化文書を復元するために必要なバージョン管理情報を圧縮処理して得られた第2の圧縮子とからなる署名データを、上記ユーザの秘密鍵で暗号化処理することによって生成されることを特徴とする電子化文書の処理システム。

【請求項18】前記検査手段が、

上記受信メッセージに含まれる電子化文書をチェック対象文書として、該チェック対象文書に所定の圧縮処理を施して文書圧縮子を生成する第1手段と、

上記受信メッセージに含まれるディジタル署名のうち、最新のものから順にチェック対象として選ばれたディジタル署名から、これと対応する復号鍵を用いて署名データを復号する第2手段と、

上記復号された署名データから抽出された第1の圧縮子と、上記チェック対象文書から生成された文書圧縮子とが一致するか否かを検査する第3手段と、

上記復号された署名データが第2の圧縮子を含む場合、上記受信メッセージに含まれるバージョン管理情報の最新のものから順にチェック対象として選び、チェック対象となったバージョン管理情報に所定の圧縮処理を施して得られた管理情報圧縮子を生成する第4手段と、

上記管理情報圧縮子と、上記復号された署名データから抽出された第2の圧縮子とが一致するか否かを検査するための第5手段と、

上記復号された署名データが第2の圧縮子を含む場合、上記チェック対象となったバージョン管理情報と上記チェック対象文書とに基づいて、前バージョンの電子化文書を復元する第6手段とを有し、

上記前バージョンの電子化文書を新たなチェック対象文書として、上記第1手段～第6手段を動作させることを

6

特徴とする請求項17に記載の電子化文書の処理システム。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、電子化文書処理システムに関し、更に詳しくは、電子化文書データに付されるディジタル署名の生成および認証のための技術に関する。

【0002】

【従来の技術】例えば、電子メールシステムを利用して、1つの文書を起案者から複数の関係者に順次に回覧し、各関係者に文書内容に対する承認を得る場合、承認した文書内容と承認者に署名との対応関係に、回覧の途中または後日に、不正な改ざんが加えられた否かを発見できるようにするため、文書データを圧縮して得たダイジェストデータ（ハッシュトータル）と承認者の個人データとを暗号化して得られる「ディジタル署名」の適用が知られている。

【0003】此種の電子化された文書データの正当性を確認するための技術は、例えば、「暗号と情報セキュリティ」、編者：辻井重男／笠原正雄、発行：昭晃堂のページ：127～147に記載の技術など、従来から種々の技術が提案されている。

【0004】図17に、ディジタル署名を利用した電子化文書の認証方法の一例を示す。

【0005】10A～10Cはネットワークを介して相互に通信する機能をもつ端末装置であり、端末装置10Aの利用者（署名者A）が文書1301を起案し、上記文書1301に署名者Aのディジタル署名SAを付した形のメッセージを端末装置10Bに送信する。端末Bの利用者（署名者B）は、受信した文書1301の内容に同意すると、端末装置10Aから受信した文書1301とディジタル署名SAに自分のディジタル署名SBを追加した形のメッセージを、文書回覧ルートにある次の端末装置10Cに送信する。ここでは、端末装置10Cの利用者Cが、上記文書に付されたディジタル署名SA、SBの正当性を確認する場合の動作を示す。

【0006】端末装置10Aにおいて、ディジタル署名SAは、次のようにして生成される。先ず、一方向の関数である圧縮関数1302aを用いて、文書データ1301の圧縮子（ハッシュトータル）を得る。得られた文書データの圧縮子と、キーボードから入力した署名者Aの個人情報（例えば、署名者Aの名前などのデータ）とで署名データ1303aを構成する。ディジタル署名SA：1306aは、上記署名データ1303aを署名者Aの秘密鍵1304aを用いて暗号化する（暗号処理1305a）ことによって得られる。

【0007】端末装置10Bにおける署名者Bのディジタル署名SBも、上記署名者Aのディジタル署名SAと同様にして、圧縮関数1302bによって圧縮された文

7

書１３０１の圧縮子と、署名者Ｂの個人情報とで構成される署名データ１３０３ｂに、署名者Ｂの秘密鍵１３０４ｂを用いた暗号処理１３０５ｂを施すことによって得られる。

【０００８】端末装置１０Ｃにおけるディジタル署名１３０６ａ、１３０６ｂの正当性の確認は次のようにして行われる。先ず、上記ディジタル署名１３０６ａ、１３０６ｂに、それぞれ署名者Ａ、Ｂの公開鍵１３０７ａ、１３０７ｂを用いた復号処理１３０８ａ、１３０８ｂを施すことによって、署名データ１３０３ａ、１３０３ｂを得る。この後、圧縮関数１３０２ｃを用いて、受信文書１３０１の圧縮子を生成し、これと署名データ１３０３ａ、１３０３ｂに含まれる文書の圧縮子とを比較する（検査関数１３０９ａ、１３０９ｂ）。

【０００９】なお、この方式では公開鍵暗号方式を使用しているため、ディジタル署名は秘密鍵を知る本人だけにしか作れず、安全性を維持できる。

【００１０】

【発明が解決しようとする課題】然るに、文書を複数の人に回覧し、各回覧先で文書内容を承認あるいは確認したことを示す署名を行う場合に、回覧途中で、既に誰かが署名済みの文書に対して、コメントの追加や誤字訂正など、文書内容の部分的変更が必要となる場合がある。また、文書中に予め部門毎の記入欄が設けてあり、複数の部門に回覧することによって完成される文書もある。

【００１１】このように、回覧の途中で内容が変化する文書に対して、上述した従来のディジタル署名を適用すると、内容変更前のバージョンの文書に付されたディジタル署名を復号化して得られる文書の圧縮子と、最新バージョンの文書データから生成した圧縮子とが一致しなくなる。

【００１２】このため、文書の最終的な確認者または回覧途中の署名者が、文書に付されたディジタル署名に対して上記端末Ｃで行った方法で認証操作した場合に、善意の基づく文書の修正あるいは更新であったにもかかわらず、文書または署名に不正があったことを示す判定結果が出されるという不都合が生ずる。

【００１３】本発明の目的は、既にディジタル署名を伴っている文書データに対して善意による内容変更を許容できるようにしたディジタル署名の生成方法およびシステムを提供することにある。

【００１４】本発明の他の目的は、それぞれバージョンの異なる文書内容と対応する複数のディジタル署名を伴った電子化文書の認証方法およびシステムを提供することにある。

【００１５】本発明の他の目的は、ディジタル署名を伴う電子化文書データを受信し、文書内容に追加あるいは部分的変更をした上で新たなディジタル署名を追加できるようにした電子化文書処理システムを提供することにある。

8

【００１６】

【課題を解決するための手段】上記の目的を達成するため、本発明に係る電子化文書処理システムでは、ネットワークから受信した既に他の署名者による少なくとも１つのディジタル署名を伴う電子化文書に対して、ユーザが文書内容の追記または変更を行なった場合に、新バージョンの電子化文書を圧縮処理して生成した文書の圧縮子と、ユーザ（署名者）の個人情報と、上記新バージョンの電子化文書から上記前バージョンの電子化文書を復元するために必要なバージョン管理情報とからなる署名データを用いて、上記ユーザのディジタル署名を生成する。上記ディジタル署名は、例えば、公開鍵暗号化法において各ユーザに割り当てられた秘密鍵を用いて、上記署名データを暗号化することによって得られる。

【００１７】上記ディジタル署名は、ネットワークから受信した前バージョンの電子化文書に付されていた他の署名者のディジタル署名と共に、上記新バージョンの電子化文書に関係付けられ、文書回覧ルートの次の人に送信される。

【００１８】本発明の電子化文書処理システムでは、回覧途中で何れかの署名者によってバージョンアップされた電子化文書を受信した場合でも、最後のディジタル署名から順に処理対象に選び、適宜、前バージョンの電子化文書への復元処理を実行しながら、ディジタル署名と電子化文書との関係をチェックすることによって、各ディジタル署名と電子化文書の正当性を認証することが可能となる。

【００１９】

【作用】ディジタル署名と電子化文書との関係チェックは、各ディジタル署名をその署名者の公開鍵で復号化することによって署名データを復元し、該署名データから抽出された文書圧縮子と、実際に受信された電子化文書を圧縮処理して得た文書圧縮子とを比較することによって行われる。

【００２０】本発明によれば、復元された署名データがバージョン管理情報を含む場合、これを用いて現在バージョンの電子化文書から１つ前のバージョンをもつ文書を復元できるため、全てのディジタル署名について、電子化文書との対応関係の確認が可能となる。

【００２１】例えば、元の電子化文書が予め定義された複数の部分領域を有し、回覧の途中で、電子化文書中のこれらの部分領域の１つに文書データを追記することによって文書のバージョンアップがなされるようになっている場合、上記バージョン管理情報として、データが新たに追記された上記部分領域の１つを特定するための情報が適用される。

【００２２】電子化文書中の任意の部分領域でデータの挿入または既存文書データの削除を行うことによって文書のバージョンアップがなされるようになっている場合、上記バージョン管理情報は、例えば、上記部分領域

9

を特定するための位置情報と、前バージョンの電子化文書から削除された文書データおよび挿入された新文書データを特定するための情報とからなる。

【００２３】バージョン管理情報は、情報量が少ない場合は、これを署名データの１部に組込、暗号化されたディジタル署名の形で、回覧ルートの他の人（端末装置）に通知できる。バージョン管理情報の情報量が多い場合は、バージョン管理情報をそのまま電子化文書の付属情報の１部として、送信すればよい。

【００２４】後者の場合、回覧途中におけるバージョン管理情報に対する不正な改変行為の有無を発見できるようにするために、例えば、バージョン管理情報を圧縮処理して得られた圧縮子を署名データに組み込み、これを暗号化処理してディジタル署名を生成するとよい。

【００２５】このようにすると、電子化文書を受信した端末装置（電子化文書処理システム）では、ディジタル署名を復号化して得られた署名データに含まれるバージョン管理情報の圧縮子と、電子化文書と共に受信したバージョン管理情報を圧縮して得た圧縮子とを照合することによって、上記バージョン管理情報が正当なものであることを確認した上で、該バージョン管理情報に基づいて、現在の電子化文書から１つ前のバージョンの電子化文書を復元することができる。

【００２６】電子化文書に順次に付されるディジタル署名には、バージョン管理情報を伴ったものと、バージョン管理情報を伴わないものとが混在していてもよい。なぜなら、電子化文書を受信した端末装置においては、最新のディジタル署名およびバージョン管理情報から順に処理対象に選び、処理対象となったディジタル署名がバージョン管理情報またはその圧縮子を含む場合にのみ、現在処理対象としているバージョン管理情報を用いて、上述した１つ前のバージョンをもつ電子化文書の復元処理を実行すればよいからである。

【００２７】

【実施例】図２は、本発明の一実施例であるディジタル署名機能を備えた複数の文書処理端末装置からなるメール通信システムの構成を示すブロック図である。図２において、１０（１０Ａ、１０Ｂ～１０Ｎ）は、通信網１２により相互に接続された端末装置であり、各端末装置１０は、後述するように、文書の作成機能と、ディジタル署名の生成および確認機能と、他の端末装置との間での通信機能をもつ。ここでは、ディジタル署名付き電子化文書データ（以下、単に文書データという）が、予め指定された文書の回覧ルートに沿って、１つの端末装置から通信網１２を介して他の端末装置に送信されるものとして説明するが、端末装置間の通信にメールサーバ２０を介在させ、各端末がメールサーバ２０をアクセスすることによって、文書データを回覧させるようにできること明らかである。

【００２８】端末装置１０は、図３に示すように、ディスプレイ１２１７と、キーボード１２１８と、各種のプログラムを格納するメモリ１２０５と、予め登録されたデータを格納するためのデータメモリ１２０６と、プログラム実行中に発生するデータを一時的に記憶するためのワークメモリ１２０７と、ＣＰＵ（中央処理装置）１２０８と、通信制御部１２０９と、Ｉ／Ｏ制御部１２１０とを備えている。

10

【００２９】上記プログラムメモリ１２０５には、複数のプログラムと、後述するディジタル署名の生成およびチェックにための複数の関数（モジュール）、具体的には、暗号処理のための関数１２１１、復号処理のための関数１２１２、データ圧縮処理のための関数（ハッシュ関数）１２１３、および認証データ検査のための関数１２１４を格納している。

【００３０】データメモリ１２０６は、電子メールシステムを利用する予め登録された複数のユーザの公開鍵を記憶するエリア１２０９と、その端末を利用するユーザの秘密鍵を記憶するエリア１２１０とを有し、これらの秘密鍵と公開鍵は、それぞれユーザの識別番号ＩＤを指定することによって読み出せるようになっている。

【００３１】図１は、上記各端末１０において行われるディジタル署名の生成方法の第１実施例を説明するための図である。ここでは、端末１０Ａにおいて利用者（署名者）Ａが作成し、利用者Ａのディジタル署名１１３Ａと、次の利用者Ｂのディジタル署名１１３Ｂとが既に付された文書データ１０１を、端末１０Ｃの利用者Ｃが受信し、上記文書の内容に部分的な変更を加えた後、利用者Ｃのディジタル署名１１３Ｃを付す手順を示す。

【００３２】この実施例で、複数の利用者に順次に回覧される文書１０１は、内容変更を許されない固定的なデータ領域１０２と、回覧先でデータが追加される追加データ領域１０３とを有する。固定データ領域１０２は、最初の署名を行う文書起案者Ａが生成した文書データを含む領域であり、最初の署名者Ａ以外の者は、受信文書の固定データ領域１０２に含まれる文書内容を変更することが許されない。２番目以降の署名者が、受信した文書１０１に予め定義されている追加データ領域１０３に適宜データの書込みを行なうことにより、文書は情報量を増しながら、順次に回覧される。ここに示した例では、文書１０１の追加データ領域１０３は３つのサブ領域に分割され、前の署名Ｂが第１番目のサブ領域にデータを追加した状態にあり、署名者Ｃは、第２番目のサブ領域にデータを追加する。

【００３３】端末１０Ｃの利用者である署名者Ｃは、先ず、受信した文書データ１０１をディスプレイ１２１７の画面に出力した状態で、キーボード１２１８を操作して、文書データの追加処理１０４を行う。これにより、追加データ領域１０３の第２番目のサブ領域にデータが追加された、更新された文書データ１０５が生成される。本発明では、各署名者が、文書データを更新した上

11

でディジタル署名を行う場合に、自分がデータ修正した個所、この実施例ではデータを追加したサブ領域を特定する情報（サブ領域番号１０８）を、バージョン管理情報として、署名データ（認証データ）の１部に含めることを特徴とする。

【００３４】文書データの更新が終わると、署名者Ｃは、更新された文書データ１０５に圧縮関数１２１３を用いて圧縮処理１０６を施し、文書圧縮子１０９を生成する。上記圧縮子１０９は、署名者Ｃの氏名等の個人情報１１０と、上述したサブ領域番号１０８と共に、署名データ１０７を構成する。上記署名データ１０７に対して、署名者Ｃに固有の秘密鍵１１１Ｃを用いて暗号処理１１２を施すことによって、文書データ１０５を署名者Ｃが承認したことを示すディジタル署名１１３Ｃが生成される。

【００３５】署名者Ｃは、上記文書データ１０５と、文書データ１０１と共に受信した他の利用者のディジタル署名１１３Ａ、１１３Ｂと、今回新たに生成した自分のディジタル署名１１３Ｃとを、図４に示す通信メッセージ１００の形式で、次の署名者（または確認者）に送る。上記各ディジタル署名１１３Ａ～１１３Ｃと後述する公開鍵との対応関係を示すために、通信メッセージ１００には、上記各ディジタル署名１１３Ａ～１１３Ｃと対をなして署名者の識別子１１４Ａ～１１４Ｃが設定される。尚、図４では、簡単化のために、通信メッセージの送信先アドレス、発信元アドレス等の情報を含むヘッダ部を省略して示してある。

【００３６】図５は、文書データを含む通信メッセージを受信した端末装置において、上述した署名動作の前処理として、あるいは回覧された文書データの最終的な確認者による署名の正当性確認のために実行される、ディジタル署名の確認処理を示す。

【００３７】ここでは、ディジタル署名１１３Ａ～１１３Ｃを含む通信メッセージ１００を受信した端末装置１０Ｄの動作を例にして説明する。端末装置１０Ｄでは、受信したメッセージから抽出した文書データ１０５に、圧縮関数１２１３を用いて、図１の処理１０６と同様の圧縮処理２０６を施し、文書の圧縮子１０９’を得る。次に、受信した通信メッセージ１００から抽出したディジタル署名１１３Ａ～１１３Ｃの内、最後のものから順にチェック対象署名とする。先ず、ディジタル署名１１３Ｃをチェック対象署名に選び、これと対をなす署名者Ｃの識別子１１４Ｃに基づいて、公開鍵記憶領域１２１６から署名者Ｃの公開鍵２１１Ｃを取りだし、この公開鍵２１１Ｃを用いて、ディジタル署名１１３Ｃに復号処理２１２を施し、署名データ２０７を得る。

【００３８】そして、上記圧縮処理２０６で得られた文書圧縮子１０９’と、署名データ２０７に含まれている文書圧縮子２０９とを検査処理２１４にかけ、これら２つの文書圧縮子が一致するかどうかを判定する。もし、

12

一致しない場合は、文書データ１０５、又はディジタル署名１１３Ｃに不正な改ざんが加えられているものと判断する。

【００３９】上記検査処理２１４によって、２つの文書圧縮子１０９’と２０９との一致が確認された場合は、署名データ２０７に含まれるサブ領域番号２０８に基づいて、文書データ１０５中の　署名者Ｃがデータを追加したサブ領域を特定し、このサブ領域に含まれるデータを削除する（文書復元処理２０４）。これによって、署名者Ｃの直前のに署名者Ｂが承認した文書データ１０１が復元される。

【００４０】上記文書データ１０１と、次のディジタル署名１１３Ｂを新たなチェック対象として、文書データ１０１の圧縮処理２０６と、ディジタル署名１１３Ｂの復号処理２１２を行い、検査処理２１４、文書の復元処理２０４を行うと、追加データ領域２０３に追加データを含まない署名者Ａが承認した文書データが復元される。従って、この文書データに上述した処理動作２０６、２１２、２１４を繰り返すことによって、ディジタル署名１１３Ａの正当性を確認することができる。以上のように、本実施例によれば、最終の署名者から順に、ディジタル署名の検査と、データ追加サブ領域番号に基づく前バージョンの文書データ復元処理を繰り返すことによって、署名者全員についてのディジタル署名の正当性の確認を行うことが可能となる。

【００４１】図６は、各端末装置１０が備える上述した文書認証およびディジタル署名を実現するためのプログラムフローチャートを示す。このフローチャートでは、端末装置が、文書の回覧ルートにおける任意順位、ｎ番目の署名者に該当するものとして、扱われている。

【００４２】前の回覧者までのｎ－１個の署名が付された文書データ（通信メッセージ）を受信すると（ステップ３０２）、ディスプレイに文書データを表示し（ステップ３０３）、図７で詳述する署名確認処理ルーチンを実行する（ステップ３０４）。上記署名確認処理ルーチンでの確認結果は、パラメータのリターン値で示される。パラメータのリターン値をチェックし（ステップ３０５）、リターン値が「１」ならば、不正な改ざんがあったものと判断し、ステップ３１４で、文書データまたは署名が正当でないことを示すメッセージをディスプレイに表示して、このプログラムを終了する。

【００４３】もし、リターン値が「０」ならば、上記文書データに付された全ての署名が正当であったと判断し、ステップ３０６で、署名が正当で合ったことを示すメッセージをディスプレイに表示し、利用者に氏名等の個人情報を入力させた後、文書への追加データの入力を許可する。ステップ３０７で、追加データ領域１０３における空き状態にあるｉ番目のサブ領域に、キーボードから入力されたコメント等の追加データを書き込み、これが終わると、ステップ３０８で、文書データに圧縮処

理を施して、文書圧縮子ｈを生成する。次に、上記ステップ３０６で入力された個人情報を変数Ｐに代入し（ステップ３０９）、変数Ｔにデータ追加サブ領域の番号ｉを代入し（ステップ３１０）、署名データＳを生成する（ステップ３１１）。署名データは、Ｓ＝（ｈ｜Ｐ｜Ｔ）で表わされる。ここで、記号「｜」は、データの連結を意味している。

【００４４】上記署名データＳに対して、署名者の秘密鍵を用いた暗号処理を施し（ステップ３１２）、ディジタル署名を生成する。そして、ステップ３１３で、今回更新された文書データ１０５と、今回受信したメッセージに含まれていた　他の利用者のディジタル署名１１３Ａ～１１３（ｎ－１）と、新たに生成した署名１１３ｎとを含む通信メッセージを編集し、次の回覧者に送信する。

【００４５】尚、文書の回覧ルートは、一般には、文書１０１中の所定の領域に文字によって表示されるが、回覧先となる各利用者の識別子とアドレスを　通信メッセージの制御情報領域に予め設定しておき、１つの端末でディジタル署名の処理が終わると、自動的に次の人にメッセージが転送されるようにしてもよい。

【００４６】図７は、署名確認処理ルーチン３０４の詳細を示すフロー図である。先ず、チェック対象となる署名の総数を示す変数ｋに、今回受信したメッセージに含まれているディジタル署名の数「ｎ－１」を代入する（ステップ３２１）。　次に、ｋ＝０か否かを判定し（ステップ３２２）、ｋ＝０となっていれば、チェックすべき署名がないと判断し、ステップ３２３へ進んで、リターンコードに「０」を設定して、図６のプログラムにリターンする。もし、ｋ≠０であれば、ｋ番目のディジタル署名に、その署名者の公開鍵を用いた復号処理を施し、署名データＳ＝（ｈ｜Ｐ｜Ｔ）を生成した後（ステップ３２４）、文書データに圧縮処理を施して圧縮子ｈ’を生成する（ステップ３２５）。次に、上記復号化された署名データに含まれる文書圧縮子ｈと、圧縮子ｈ’とを比較する（ステップ３２６）。

【００４７】もし、ｈ≠ｈ’ならば、不正な改ざんが行なわれていると判断し、ステップ３２９に進んで、リターンコードに「１」を設定し、図６のプログラムにリターンする。もし、ｈ＝ｈ’ならば、正当な署名であると判断し、上記復号化された署名データに含まれる位置情報Ｔに基づいて、文書の追加データ領域のＴ番目のサブ領域に書かれたデータを削除した後（ステップ３２７）、変数ｋの値から１を引き（ステップ３２８）、判定ステップ３２２に戻る。

【００４８】なお、このルーチンでは、ステップ３２７を繰り返すことによって、文書データが順次に前のバージョンに戻っていくが、次の署名者に送信すべき最新の文書データそのものは、別の記憶エリアに保存されており、このルーチンを実行することによって回覧すべき文書データが損なわれることはない。

【００４９】本実施例によれば、各署名者は回覧されてきた文書にコメント等の付加データを追加することができる。また、このようなデータの追加によって、ディジタル署名の対象となる文書が回覧途中で変形されても、本発明によれば、各ディジタル署名と対応するバージョンの文書データを復元できるため、正当な署名を誤って不当な署名と誤診するおそれはない。

【００５０】図８は、本発明によるディジタル署名の生成方法の第２の実施例を示す。この例では、署名者Ｂは、文書の起案者Ａから受信した文書データ４０１の任意の領域において文書内容に変更を加え（文書変更処理４０２）、更新された文書データ４０３に対してディジタル署名を行う。署名者Ｂが受信文書に対して行った変更（データ追加、データの置換あるいは削除）の内訳は、図１０で説明するバージョン管理テーブル（文書変更／更新管理テーブル）４１２に記録され、更新された文書データと共に、次の署名者に送信される。

【００５１】ディジタル署名は、次のようにして行われる。更新された文書データ４０３に圧縮処理４０４を施し、文書圧縮子４０７を生成する。また、バージョン管理テーブル４１２に圧縮処理４１３を施し、バージョン管理テーブル４１２Ｂの圧縮子４０６を生成する。署名データ４０５は、これらの圧縮子４０６、４０７と、署名者Ｂの氏名等の個人情報４０８とからなる。上記署名データ４０５に対して、署名者Ｂの秘密鍵４０９Ｂを用いた暗号処理４１０を施し、ディジタル署名４１１Ｂを生成する。

【００５２】更新された文書データ４０３と、バージョン管理テーブル４１２Ｂと、ディジタル署名４１１Ｂは、それ以前のディジタル署名４１１Ａとともに、図９のに示すような通信メッセージ４００の形式で、次の署名者（または確認者）に送信される。なお、受信した文書の内容の１部が、前の何れかの署名者Ｎによって既に更新されている場合、後の署名者Ｍによって新たに生成されたバージョン管理テーブル４１２Ｍは、既に存在するバージョン管理テーブル４１２Ｎに続く形で、通信フレームに挿入される。

【００５３】バージョン管理テーブル４１２は、図１０に示すように、データ変更が施された領域毎に生成される複数のレコード５０５、５０６、……からなる。各レコードは、データ変更の種類を示すコードを記憶するためのフィールド５０１と、文書中におけるデータ変更が施された部分領域の先頭位置を示すアドレスを記憶するためのフィールド５０２と、文書変更処理４０２で上記領域に新たに挿入されたデータのサイズを記憶するための５０３と、文書変更処理４０２で上記領域から削除されたデータを記憶するためのフィールド５０４とを含む。

【００５４】フィールド５０１に設定されるコードの値

15

と処理内容との関係は、次のようになっている。

「１」：データの追加、「２」：データの置き換え、「３」：データの削除。

【００５５】図１０に示した例において、例えば、レコード５０５は、受信した文書中のアドレス「２７９１２０」から部分領域に存在していた旧データ「ｕｊｉ８……８ｙｌ」を長さ「３２００」キャラクタの新たなデータに置き換えたことを意味する。上記新たなデータは、更新された文書４０３に存在している。レコード５０６は、受信文書中のアドレス「８９１２３６」から始まる部分領域に長さ「４５８」キャラクタのデータが挿入されたことを意味し、レコード５０７は、アドレス「１１４０３１」から始まる部分領域にあったデータ「ｋｈｔ…４５ｏｊ」が削除されたことを意味している。

【００５６】図１１は、上述したバージョン管理テーブル４１２を伴う文書データを受信した端末装置１０Ｃで行われるディジタル署名の正当性確認の手順を示す。まず、受信メッセージから抽出した文書データ４０３に圧縮処理６０４を施すことによって、文書の圧縮子４０７’を生成する。次に、受信メッセージから抽出したディジタル署名４１１Ｂに対して、署名者Ｂの公開鍵６０９Ｂを鍵として復号処理６１０を施し、署名データ６０５を生成する。上記圧縮処理６０４で得た文書の圧縮子４０７’と署名データ６０５に含まれる文書の圧縮子６０７とを比較し（検査処理６１２）、２つの文書圧縮子が一致するか否かを判定する。もし、これらが一致しない場合は、文書データ４０３またはディジタル署名４１１Ｂに不正な改ざんが加えられているものと判断する。

【００５７】上記２つの文書圧縮子の一致が確認された場合は、受信メッセージから抽出した署名者Ｂのバージョン管理テーブル４１２Ｂに圧縮処理６１４を施し、テーブル圧縮子４０６’を生成する。得られたテーブル圧縮子４０６と、署名データ６０５に含まれているテーブル圧縮子６０６とを比較し（検査処理６１５）、これらの圧縮子が一致するか否かを判定する。もし、これらが一致しないときは、バージョン管理テーブル４１２Ｂまたはディジタル署名４１１Ｂに不正な改ざんが加えられたものと判断する。

【００５８】上記２つのテーブル圧縮子の一致が確認された場合は、バージョン管理テーブル４１２Ｂの各レコードの内容に基づいて、文書データ４０３に復元処理６０２を施し、署名者Ａが承認したバージョンの文書データ４０１を得る。

【００５９】上記復元処理６０２では、バージョン管理テーブル６１３の各レコードに示されたコード５０１に従って、追加された部分データの文書データ４０３からの削除（コードが「１」または「２」の場合）と、削除されたデータ５０４の文書データ４０３への挿入（コードが「２」または「３」の場合）とが行なわれる。

【００６０】このようにして復元された文書データ４０

16

１と、受信メッセージから抽出された署名者Ａのディジタル署名４１１Ａを対象として、上述した処理を繰り返すことによって、ディジタル署名４１１Ａの正当性チェックすることができる。

【００６１】以上の如く、本実施例によれば、最終の署名者から順に、ディジタル署名の正当性チェックと、前バージョンの文書データの復元処理を繰り返すことによって、回覧の途中で文書の任意の部分で内容更新がなされた場合でも、全ての署名者のディジタル署名の正当性を確認することができる。

【００６２】図１２は、図８に示したディジタル署名の生成方法の変形例を示す。この実施例では、文書の起案者は、文書の圧縮子と個人情報とからなる署名データを暗号処理してディジタル署名を生成し、２番目以降の署名者は、更新管理テーブル４の圧縮子４０６と、署名者の個人情報４０８とで署名データ４０５’を構成し、文書の圧縮子を含まない署名データ４０５’に対して署名者Ｂの秘密鍵４０９Ｂを用いた暗号処理４１０を施すことによって、ディジタル署名４１１Ｂ’を生成するようにしたものである。

【００６３】このディジタル署名の作成方法は、例えば、回覧先の各署名者毎に文書中の特定のコメント領域が割り当てられ、各署名者が文書の一部を必ず更新するような構造をもつ文書に対して有効となる。

【００６４】図１３は、図１２に示した方法で生成されたディジタル署名をもつ文書データを受信した端末装置１０Ｃで行われる２番目以降のディジタル署名の正当性確認の手順を示す。文書データの圧縮子の生成と検査（図１１における処理６０４と６１２）が省略されている点を除いて、図１１で説明した動作と同様の動作が行われている。最初の署名者に関しては、図１１に示したように、文書を圧縮処理して得た圧縮子と、署名データから抽出した文書圧縮子との比較によって、その正当性をチェックする。

【００６５】本実施例によれば、文書の圧縮子に関する検査を１部省略できるため、認証動作を高速化することができる。

【００６６】図１４は、バージョン管理テーブル４１２の変形例９００を示す。ここに示したバージョン管理テーブル９００は、複数の署名者に共用されるもので、各レコード９０７～９１１は、署名者の個人識別子を記憶するフィールド９０１と、更新処理の種類を示すコードを記憶するためのフィールド９０２と、文書中におけるデータ変更が施された部分領域の先頭位置を示すアドレスを記憶するためのフィールド９０３と、文書変更処理４０２で上記領域に新たに挿入されたデータのサイズを記憶するための９０４と、文書変更処理４０２で上記領域から削除されたデータを記憶するためのフィールド９０５と、ディジタル署名を記憶するためのフィールド９０６とからなる。

17

【００６７】最初の署名者である文書データの起案者は、レコード９０７に示すように、個人識別子と、文書更新がないことを示すコード「０」と、ディジタル署名とをテーブルに登録する。

【００６８】受信した文書データに部分的な変更を加えた署名者は、修正個所毎にレコードを生成し、各レコードに個人識別子分と、図１０で説明したのと同様の定義に従ってバージョン管理情報（９０２～９０５）を登録する。複数の部分領域に対してデータ修正を施した署名者は、最後のレコードのフィールド９０６にディジタル署名を登録する。文書の起案者以外の署名者で、受信した文書データに変更を加えなかった者は、例えばレコード９１０に示すように、署名者の個人識別情報と、コード「０」と、ディジタル署名とを登録する。

【００６９】上記バージョン管理テーブル形式を採用した場合、各端末が送受信する通信メッセージは、最新の文書データと、それに続くバージョン管理テーブルとからなるフレームフォーマットとなる。

【００７０】図１５は、図１で説明したディジタル署名生成方法の変形例を示す。この例では、文書の圧縮処理１００６で処理対象とする文書領域を２つに分け、文書１０５の固定データ領域１０２に含まれるデータの圧縮子１０１０と、追加データ領域１０３に含まれるデータの圧縮子１００９とを別個に生成する。これらの圧縮子１００９、１０１０と、個人情報１０１１と、サブ領域番号１０８とで署名データ１００７を構成し、これの署名データに対して、署名者Ｃの秘密鍵１１１Ｃを用いた暗号処理１１２を施し、ディジタル署名１０１３Ｃを作成する。

【００７１】図１６は、上述したディジタル署名１０１３Ｃを伴う文書データを受信した端末装置１０Ｄで行われる署名の確認手順を示す。端末装置１０Ｄは、受信メッセージから抽出した文書データ１０５に圧縮処理２００６を施し、固定データ領域１０２に含まれるデータの圧縮子１０１０’と、追加データ領域１０３に含まれるデータの圧縮子１００９’とを生成する。また、上記受信メッセージから抽出されたディジタル署名１０１３Ｃに、署名者Ｃの公開鍵２１１Ｃを用いて復号処理２１２を施すことによって署名データ２００７を得る。

【００７２】ディジタル署名１０１３Ｃの正当性は、固定データ領域１０２に関するデータ圧縮子１０１０’と署名データ２００７に含まれるデータ圧縮子２０１０との一致、および、追加データ領域１０３に関するデータ圧縮子１００９’と署名データ２００７に含まれるデータ圧縮子２００９との一致をそれぞれ検査処理２０１４でチェックすることによって行う。

【００７３】本実施例によれば、ディジタル署名に異常が検出された時、文書データの改ざん個所が、固定データ領域１０２と追加データ領域１０３の何れにあるかを特定できる利点がある。

18

【００７４】なお、上述した全てのディジタル署名の生成方法は、文書データの種別（テキスト、図形、音声、画像、またはそれらを合成したもの）に依らず適用可能である。

【００７５】

【発明の効果】以上の説明から明らかなように、本発明によれば、バージョン管理情報を用いたことによって、現在の文書データから順次に１つずつ前のバージョンの文書データを復元できるため、回覧の途中で、文書データの１部に不正でないデータの追加、変更などの処理が加わった場合でも、各署名者のディジタル署名と、その前提となる文書データとの対応関係を間違いなく認証することができる。

【図面の簡単な説明】

【図１】本発明によるディジタル署名生成手順の第１の実施例を説明するための図。

【図２】本発明を適用する複数の端末からなる電子メールシステムの全体構成を示す図。

【図３】端末装置の構成を示すブロック図。

【図４】第１実施例における通信メッセージの構成を示す図。

【図５】第１の実施例におけるディジタル署名の確認手順を説明するための図。

【図６】ディジタル署名の確認と生成を行うためのプログラムフローチャート。

【図７】図６における署名確認処理ルーチン３０４の詳細を示すフローチャート。

【図８】本発明によるディジタル署名生成手順の第２の実施例を説明するための図。

【図９】第２実施例における通信メッセージの構成を示す図。

【図１０】バージョン管理テーブルの構造を示す図。

【図１１】第２の実施例におけるディジタル署名の確認手順を説明するための図。

【図１２】本発明によるディジタル署名作成手順の第３の実施例を説明するための図。

【図１３】第３の実施例におけるディジタル署名の確認手順を説明するための図。

【図１４】バージョン管理テーブルの変形例を示す図。

【図１５】本発明のディジタル署名生成手順の第４の実施例を説明するための図。

【図１６】第４の実施例におけるディジタル署名の確認手順を説明するための図。

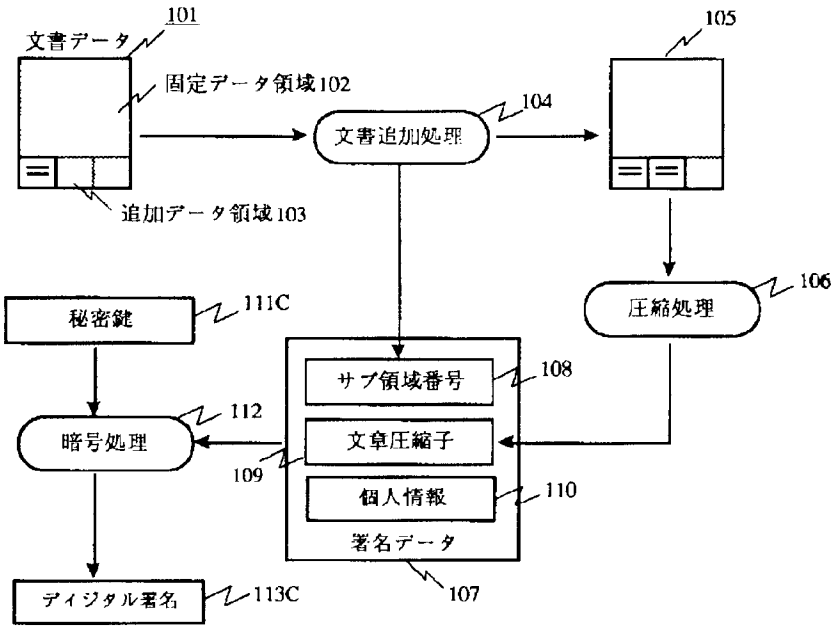
【図１７】従来のディジタル署名の処理方法を説明するための図。

【符号の説明】

１０１…元の文書データ、１０５…新バージョンの文書データ、１０７…署名データ、１０８…バージョン管理情報、１１１…秘密鍵、１１３…ディジタル署名、２１１…公開鍵、２０７…ディジタル署名。

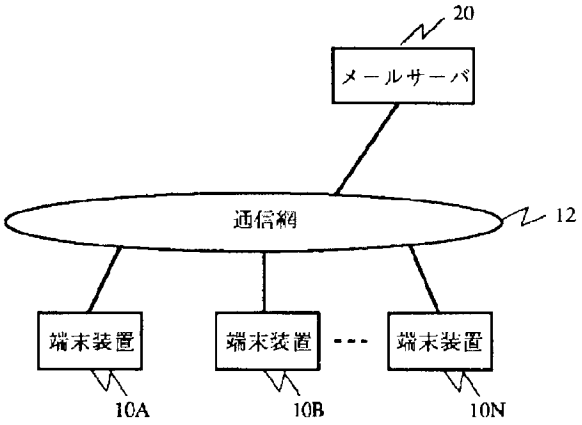
【図１】

図　1



【図２】

図　2



【図１０】

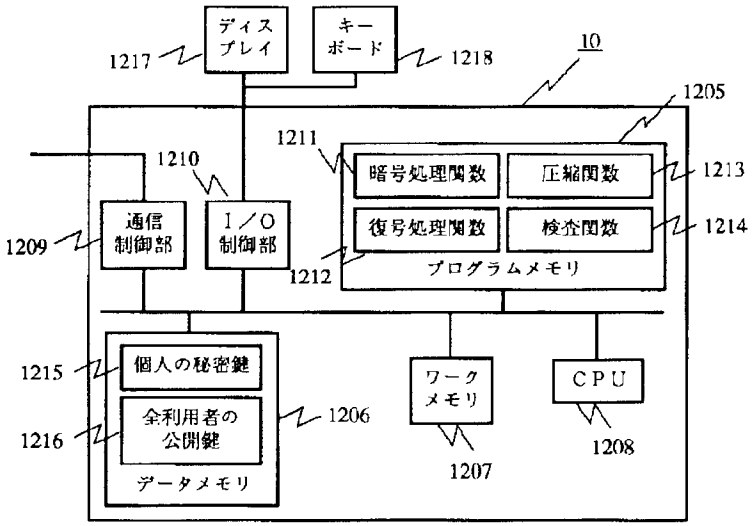
図　１０

501 コード	502 アドレス	503 サイズ	504 データ
505 2	279120	3200	ujr8t3qhlivha…wef8yhaf8yl
506 1	891236	458	—
507 3	114031	—	khtp0u65poj…retu9iyw45oj
⋮	⋮	⋮	⋮

バージョン管理テーブル 412

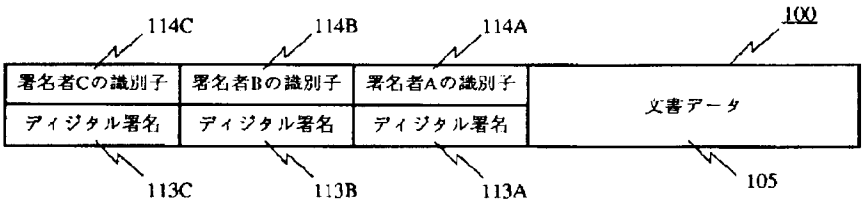
【図３】

図　3


ディスプレイ
キーボード
1217
1218
10
1205
1211
1210
暗号処理関数
圧縮関数
1213
1209
通信制御部
I／O制御部
復号処理関数
検査関数
1214
1212
プログラムメモリ
1215
個人の秘密鍵
全利用者の公開鍵
1216
1206
データメモリ
ワークメモリ
1207
CPU
1208

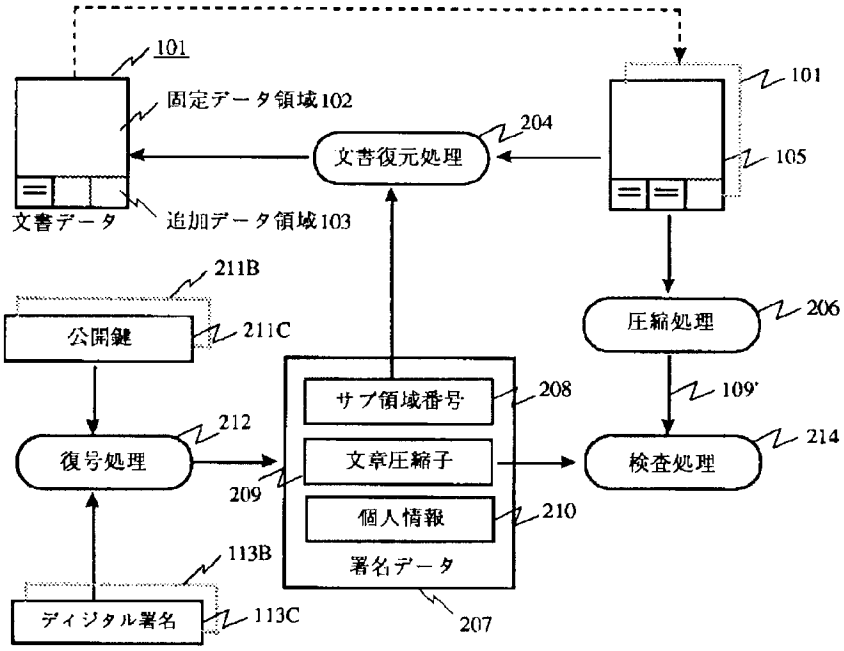
【図４】

図　4


114C
114B
114A
100
署名者Cの識別子
署名者Bの識別子
署名者Aの識別子
文書データ
ディジタル署名
ディジタル署名
ディジタル署名
113C
113B
113A
105

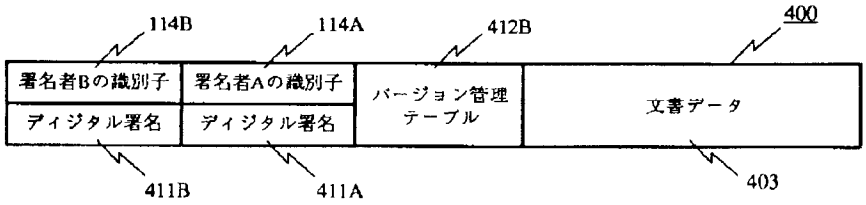
【図５】

図　５


101
固定データ領域102
文書データ
追加データ領域103
204
文書復元処理
101
105
211B
公開鍵
211C
圧縮処理
206
サブ領域番号
208
109'
212
復号処理
文章圧縮子
214
検査処理
209
個人情報
210
署名データ
113B
ディジタル署名
113C
207

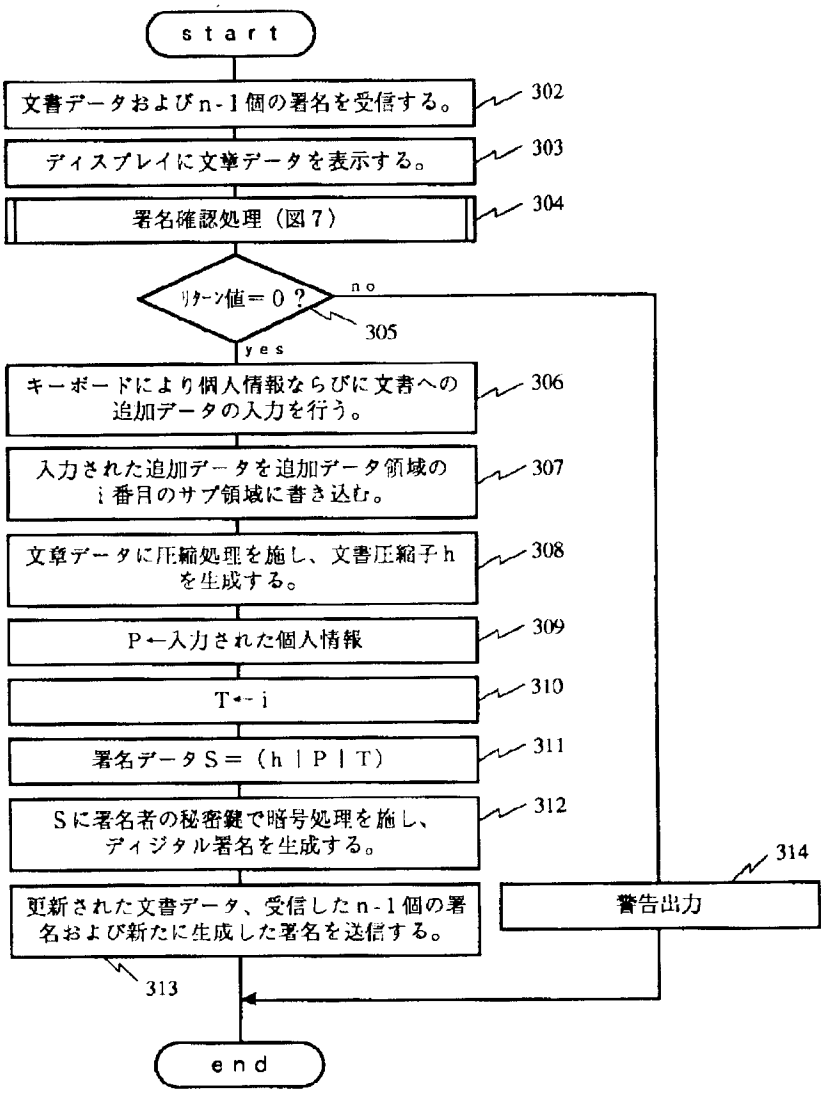
【図９】

図　９


114B
114A
412B
400
署名者Bの識別子
署名者Aの識別子
バージョン管理テーブル
文書データ
ディジタル署名
ディジタル署名
411B
411A
403

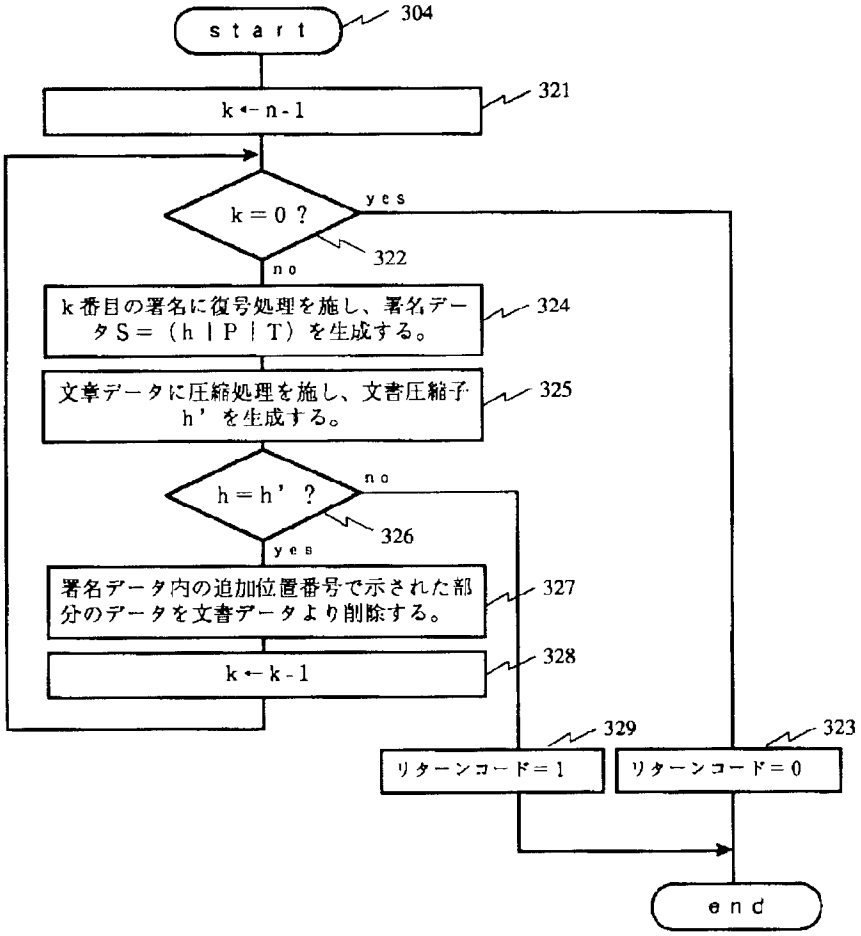
【図６】

図　6


start
文書データおよびn-1個の署名を受信する。
302
ディスプレイに文章データを表示する。
303
署名確認処理（図7）
304
リターン値＝0？
no
305
yes
キーボードにより個人情報ならびに文書への追加データの入力を行う。
306
入力された追加データを追加データ領域のi番目のサブ領域に書き込む。
307
文章データに圧縮処理を施し、文書圧縮子hを生成する。
308
P←入力された個人情報
309
T←i
310
署名データS＝（h｜P｜T）
311
Sに署名者の秘密鍵で暗号処理を施し、ディジタル署名を生成する。
312
更新された文書データ、受信したn-1個の署名および新たに生成した署名を送信する。
313
警告出力
314
end

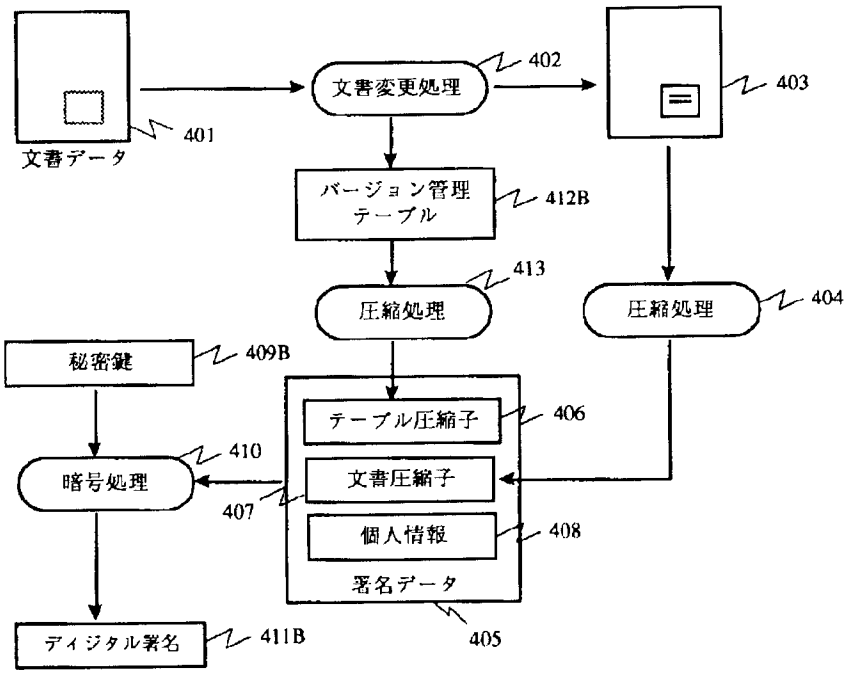
【図７】

図　7


start
304
k←n-1
321
k＝0？
yes
322
no
k番目の署名に復号処理を施し、署名データS＝（h｜P｜T）を生成する。
324
文章データに圧縮処理を施し、文書圧縮子h'を生成する。
325
h＝h'？
no
326
yes
署名データ内の追加位置番号で示された部分のデータを文書データより削除する。
327
k←k-1
328
リターンコード＝1
329
リターンコード＝0
323
end

【図８】

図　８



【図１４】

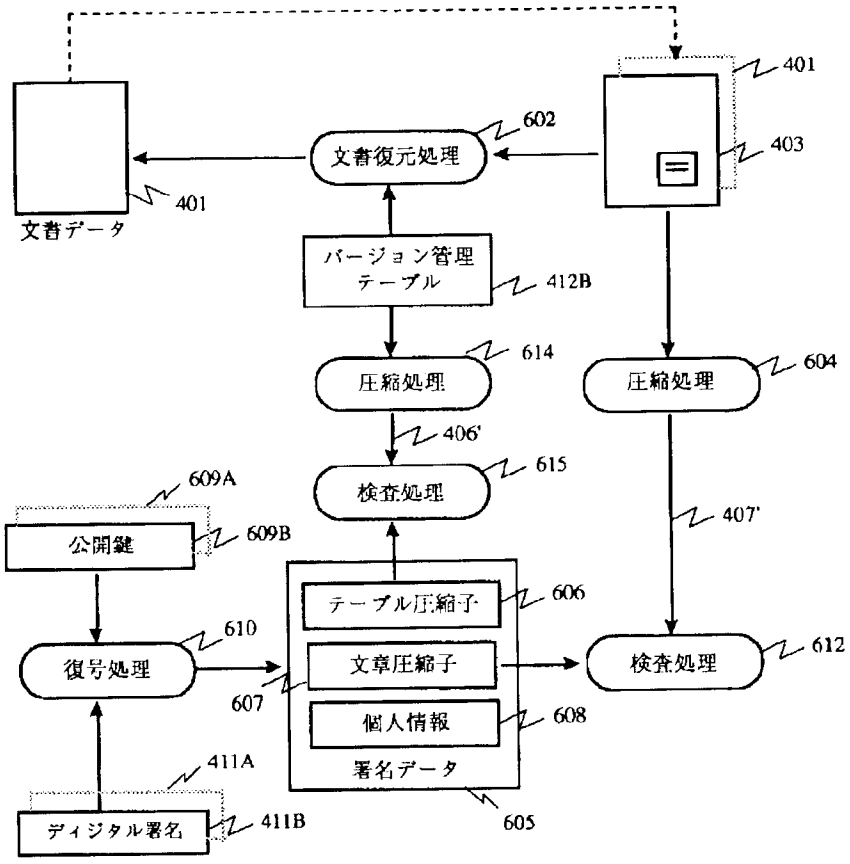
図　１４

	901 個人ＩＤ	902 コード	903 アドレス	904 サイズ	905 データ	906 ディジタル署名
907	A	0	—	—	—	1101…010
908	B	2	279120	3200	wjr8:3qhl…yhaOkyl	—
909	B	1	891236	458	—	1000…110
910	C	0	—	—	—	0100…110
911	D	3	114031	—	khtp0u65…riyw45oj	0111…010
	⋮	⋮	⋮	⋮	⋮	⋮

バージョン管理テーブル 902

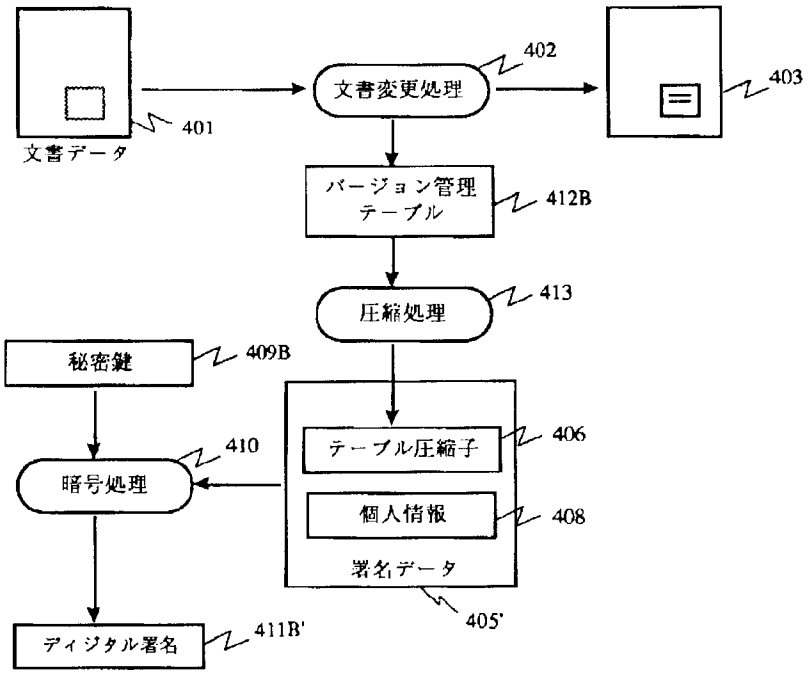
【図１１】

図　１１


401
602
文書復元処理
403
401
文書データ
バージョン管理
テーブル
412B
614
圧縮処理
604
圧縮処理
406'
615
検査処理
609A
407'
公開鍵
609B
テーブル圧縮子
606
610
復号処理
文章圧縮子
612
検査処理
607
個人情報
608
署名データ
411A
ディジタル署名
411B
605

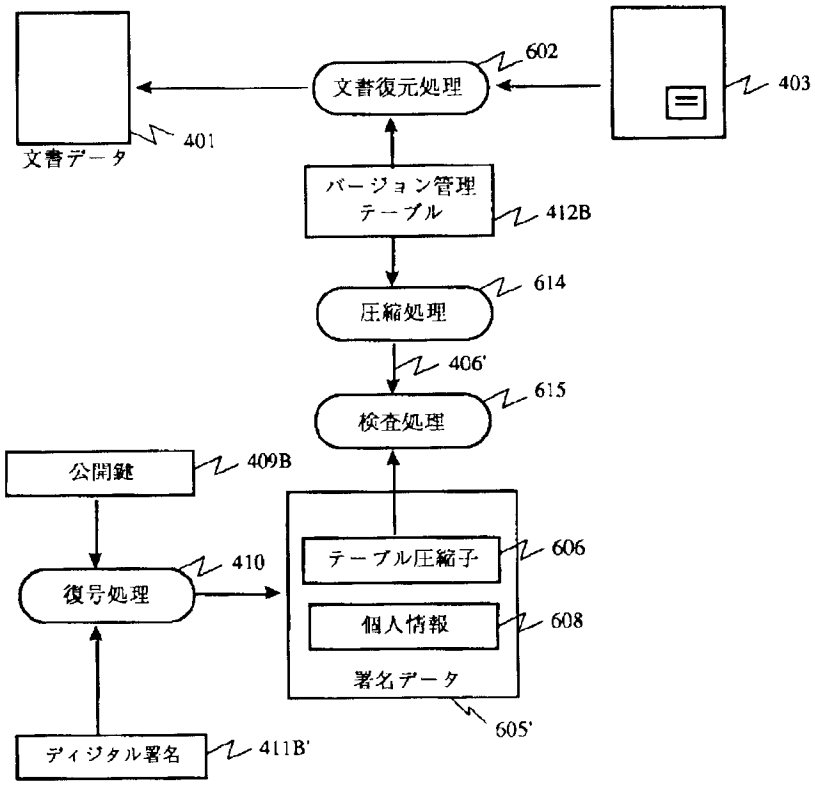
【図１２】

図　１２


文書データ
401
文書変更処理
402
403
バージョン管理
テーブル
412B
圧縮処理
413
秘密鍵
409B
テーブル圧縮子
406
暗号処理
410
個人情報
408
署名データ
405'
ディジタル署名
411B'

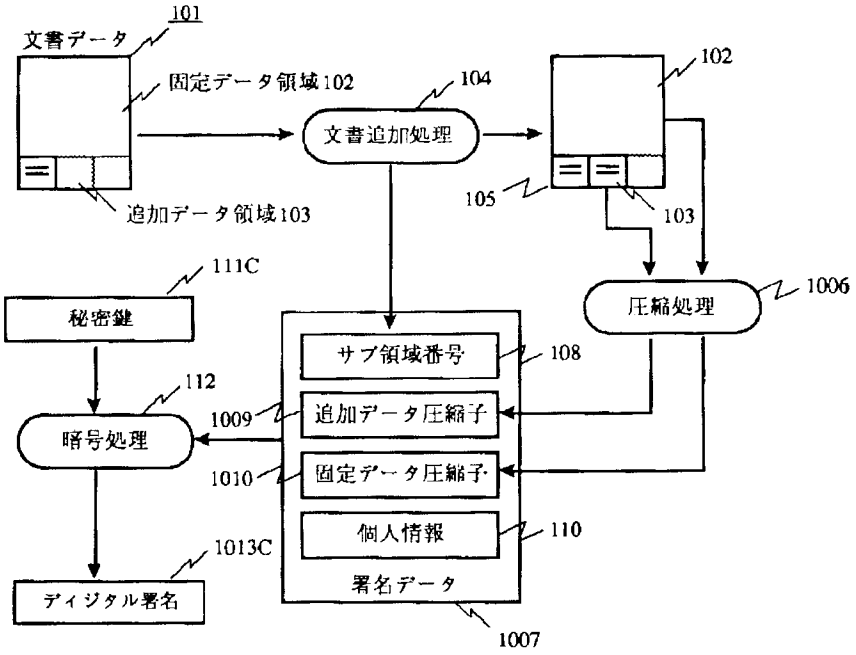
【図１３】

図　１３


602
文書復元処理
403
401
文書データ
バージョン管理
テーブル
412B
614
圧縮処理
406'
615
検査処理
公開鍵
409B
テーブル圧縮子
606
410
復号処理
個人情報
608
署名データ
605'
ディジタル署名
411B'

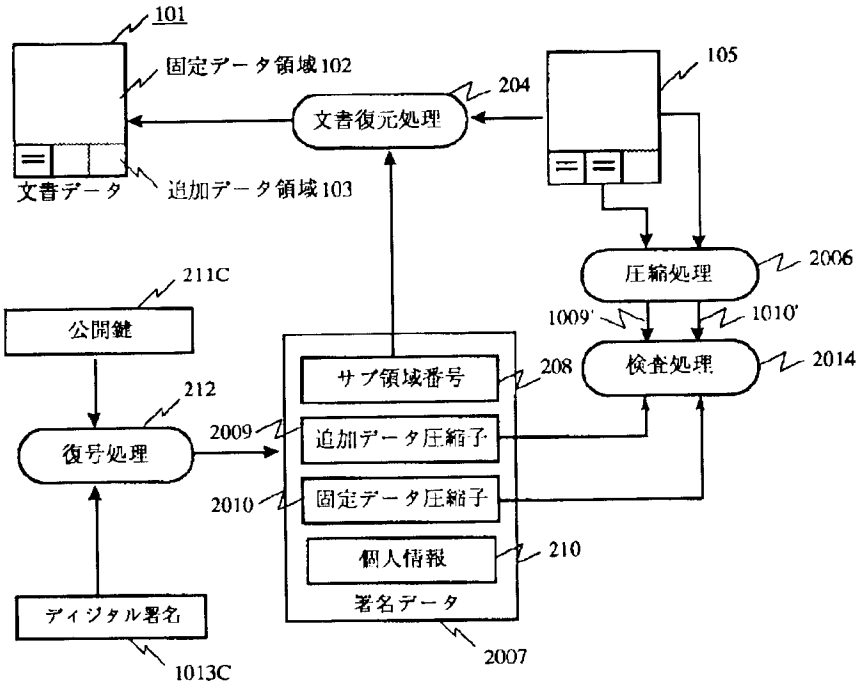
【図１５】

図　１５


101
文書データ
固定データ領域102
104
文書追加処理
102
追加データ領域103
105
103
111C
秘密鍵
圧縮処理
1006
サブ領域番号
108
112
1009
追加データ圧縮子
暗号処理
1010
固定データ圧縮子
個人情報
110
1013C
ディジタル署名
署名データ
1007

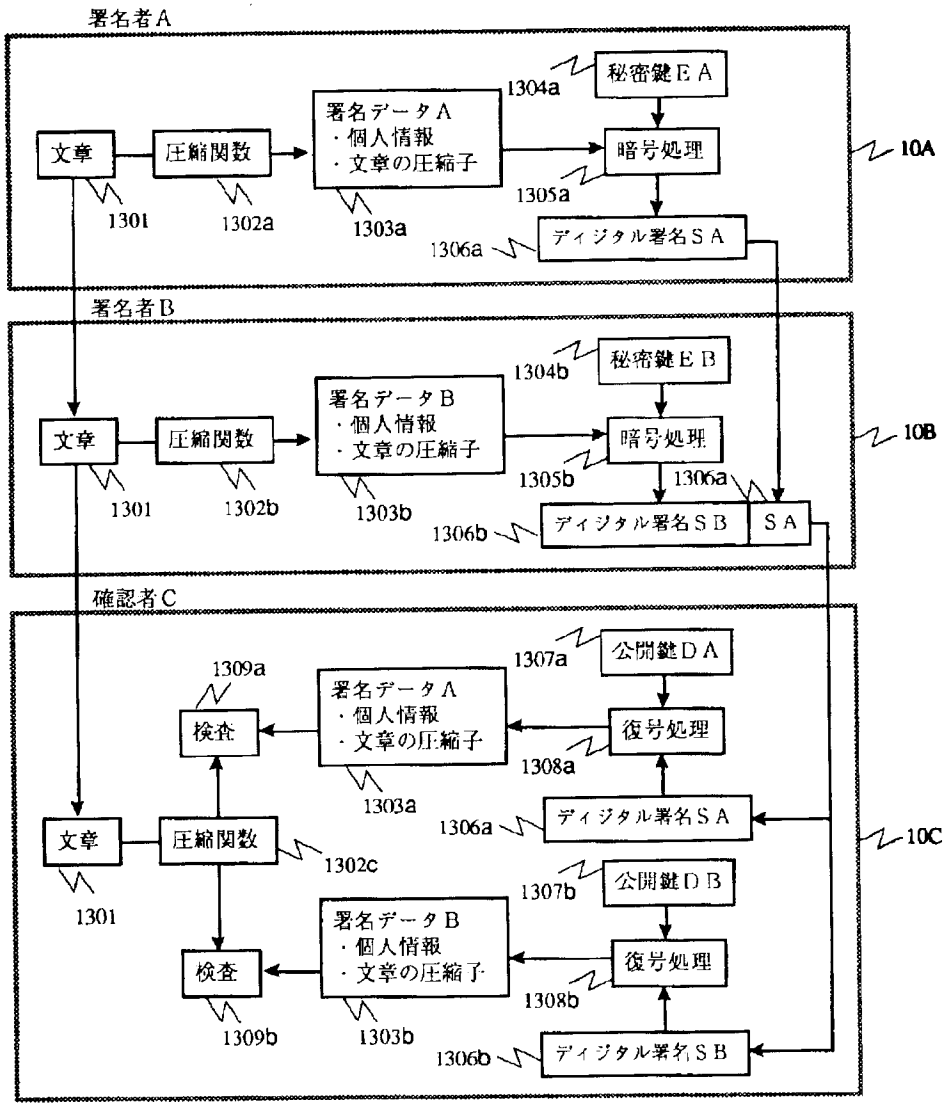
【図１６】

図　１６


101
固定データ領域102
文書データ
追加データ領域103
204
文書復元処理
105
圧縮処理
2006
1009'
1010'
検査処理
2014
211C
公開鍵
212
復号処理
2009
2010
サブ領域番号
208
追加データ圧縮子
固定データ圧縮子
個人情報
210
署名データ
2007
ディジタル署名
1013C

【図１７】

図　１７



フロントページの続き

(72)発明者　洲崎　誠一
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(72)発明者　前澤　裕行
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(72)発明者　小泉　忍
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】平成１３年４月６日（２００１．４．６）

【公開番号】特開平６－２２４８９６
【公開日】平成６年８月１２日（１９９４．８．１２）
【年通号数】公開特許公報６－２２４９
【出願番号】特願平５－３０３７７３
【国際特許分類第７版】
H04L 9/00
9/10
9/12
G09C 1/00
【ＦＩ】
H04L 9/00 Z
G09C 1/00

【手続補正書】
【提出日】平成１２年４月５日（２０００．４．５）
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】発明の名称
【補正方法】変更
【補正内容】
【発明の名称】ディジタル署名の生成方法
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正内容】
【特許請求の範囲】
【請求項１】少なくとも１つのディジタル署名が関係付けられている前バージョンの電子化文書について、文書データの追記または変更を行なって新バージョンの電子化文書を作成し、上記新バージョンの電子化文書を圧縮処理して文書の圧縮子を生成し、上記文書圧縮子と、署名者の個人情報と、上記新バージョンの電子化文書から上記前バージョンの電子化文書を復元するために必要なバージョン管理情報とを含む署名データを暗号化処理して、新たなディジタル署名を生成し、上記新バージョンの電子化文書に、上記前バージョンの電子化文書に関係付けられていたディジタル署名と上記新たなディジタル署名とを関係付けることを特徴とするディジタル署名の生成方法。
【請求項２】前記署名データの暗号化処理が、公開鍵暗号化法において前記署名者に割り当てられた秘密鍵を用いて行われることを特徴とする請求項１に記載のディジタル署名の生成方法。
【請求項３】前バージョンの電子化文書が、データを追記するために用意された予め定義された複数の部分領域を有し、前記新バージョンの電子化文書が、前バージョンの電子化文書中の上記部分領域の１つに文書データを新たに追記することによって生成され、前記バージョン管理情報は、文書データが新たに追記された上記部分領域の１つを特定するための情報からなることを特徴とする請求項１に記載のディジタル署名の生成方法。
【請求項４】前記文書圧縮子が、前記新バージョンの電子化文書中の前記複数の部分領域に含まれる文書データを圧縮処理して得られる第１の圧縮子と、前記新バージョンの電子化文書中のその他の領域に含まれる文書データを圧縮処理して得られる第２の圧縮子とからなることを特徴とする請求項３に記載のディジタル署名の生成方法。
【請求項５】前記新バージョンの電子化文書が、前バージョンの電子化文書中の少なくとも１つの部分領域での新文書データの挿入または既存文書データの削除を行うことによって生成され、前記バージョン管理情報が、上記部分領域の位置と、前バージョンの電子化文書から削除された文書データおよび挿入された新文書データを特定するための情報とからなることを特徴とする請求項１に記載のディジタル署名の生成方法。